# Web Articles

There are articles on the Internet, **not published in printed form**, that are closely related to this work.

## Web Documents

| Name | Publication Date | Abstract |
|---|---|---|
| Risk in the Balance | 1/01/05 | An effective application-security strategy today must include provision for software vulnerability detection and assessment during the software development process. This practice significantly reduces the risk that vulnerabilities will make it into production – and become corporate liabilities. |
| Security in the Software Development Lifecycle - An introduction to CLASP, the Comprehensive Lightweight Application Security Process | 1/01/05 | Application security is an important emerging requirement in software development. Beyond the potential for severe brand damage, potential financial loss and privacy issues, risk-aware customers such as financial institutions and governmental organizations are looking for ways to assess the security posture of products they build or purchase, and plan to ultimately hold vendors accountable for security problems in their software. This problem is further exacerbated by perceived security risks associated with the growing adoption of outsourced development, as well as free or open source software. |
| Security Metrics Guide for Information Technology Systems | 1/07/03 | This document provides guidance on how an organization, through the use of metrics, identifies the adequacy of in-place security controls, policies, and procedures. It provides an approach to help management decide where to invest in additional security protection resources or identify and evaluate nonproductive |

| | | |
|---|---|---|
| | | controls. It explains the metric development and implementation process and how it can also be used to adequately justify security control investments. The results of an effective metric program can provide useful data for directing the allocation of information security resources and should simplify the preparation of performance-related reports. |
| The CLASP Application Security Process | 1/01/05 | *The CLASP Application Security Process*, by Secure Software, Inc. |
| The Trustworthy Computing Security Development Lifecycle | 1/03/05 | This paper discusses the Trustworthy Computing Security Development Lifecycle (or SDL), a process that Microsoft has adopted for the development of software that needs to withstand malicious attack. The process encompasses the addition of a series of security-focused activities and deliverables to each of the phases of Microsoft's software development process. These activities and deliverables include the development of threat models during software design, the use of static analysis code-scanning tools during implementation, and the conduct of code reviews and security testing during a focused "security push". Before software subject to the SDL can be released, it must undergo a Final Security Review by a team independent from its development group. When compared to software that has not been subject to the SDL, software that has undergone the SDL has experienced a significantly reduced rate of external discovery of security vulnerabilities. This paper describes the SDL and discusses experience with its implementation across Microsoft software. (19 printed pages) |

|  |  |  |
|---|---|---|
| Why Application Security Is The New Business Imperative and How to Achieve It | 1/01/05 | Businesses are being held increasingly accountable for the security of their business applications – by customers, business partners and government. Beyond compliance costs, poor application security can result in heavy downstream remediation and management costs, not to mention productivity problems, hits on revenue and damage to corporate reputations. |